

Privacy Laws and Security Breaches in Identity Management Systems

Aashish Bhardwaj¹ and Sarvottam Dixit²

¹Research Scholar, Mewar University, Chittorgarh, Rajasthan

²Supervisor, Mewar University, Chittorgarh, Rajasthan

(E-mail: aashish.bhardwaj@gmail.com)

Abstract – With the invent of internet and increasing use of social media, incidents of identity breaches has increased. The paper defines the identity management, its features and its role in increasing security and productivity while decreasing cost, downtime and repetitive tasks. It defines privacy laws of different countries like India, Japan, Mexico, Argentina, United Kingdom and United States. Challenges for users and business in implementing identity management systems are also presented.

Keywords – Privacy, Identity Management, Security

I. INTRODUCTION

An identity is considered as a unique name entity within a system. This entity interacts within the system or from outside [1]. Identity management systems are used to authenticate entities with different permissions to interact and access resources. It is necessary as organization is bound to provide its customers required services precisely and reliably. A good identity management system increases the trust of customers, integrity, scalability mechanisms, regulations and laws for organization. The system also includes identity theft where customer's identity is purposely used by others to gain financial or social advantages. These include theft related to social gains, income disclosures, health records, age related records etc.

Security is one of the key factors seen by customers which are possibility of no or absolute minimum risks [2]. Security is related important aspects of data, hardware and software which are of prime concern to customers. Customer requirements for the security are access control, hardware protection, denial of service attack, protection from natural disasters etc.

Components of Identity management are modular and have multiple services [3]. Figure 1 shows cycle of Identity management and components are explained as:

- **User Account Repository:** There is a centralized repository of accounts with user information. This can

be accessed by different systems and thus provide a central control of user accounts.

- **Auditing:** All user accesses are controlled and monitored for security purpose. This is most of the time when some impeachments happen in organization which leads to financial or other losses.
- **Single Sign-On:** Identity management enables a technology which allows user to sign-on once in the system. Then all applications are accessed with further authentication.
- **Authentication:** Using data residing in central repository, the system authenticate users for their credentials. This is a step towards restricting unwanted people to enter in network.
- **Federation:** This includes an external users or group which is provided with delegated user management. This is used as a trusted partner between two unknown persons or organizations.
- **Authorization Management:** This is a system by group to manage user access for resources. It is defined for policy definition and implementation to where requests are approved or rejected.
- **Delegation:** A user or a group of users delegate a user for associated workflow, review or approval purposes. This includes mainly time-based access where responsibility is shared.

II. PRIVACY LAWS AND SECURITY BREACHES IN IDENTITY MANAGEMENT

In today's mobile, internet and cloud based environment; a new era of identity and access risk management is identified.

The challenges inherent to adoption of identity management systems have been presented and found a deeper business insight. The right mix of cloud analytics solutions will be assisted by the departments for particular Business Intelligence

needs. Evaluating different cloud approaches it is also found that Hybrid or mix-cloud approach is best solution for security and availability issues. An important role is also played by the feedback based updations of Business Intelligence products. Overall analytic solutions will reduce ease of usage and cost reduction. With the adoption of new technologies and rapid development a huge volume of data is acquired. This data is resulted from daily transactions, customer feedbacks, monitoring, website tracking, blogs and tweets. For analyzing this data, different products have been developed. Some of these are BIME, Birst, GoodData, Oracle Exalytics, Power BI, SAP Lumira, Tableau, TIBCO Spotfire, Vertica and Watson Analytics.

Some of the countries and their privacy laws are mentioned in the Table 1.

TABLE 1: PRIVACY LAWS OF DIFFERENT COUNTRIES

S. No.	Country	Privacy Law
1	Argentina (http://unpan1.un.org)	Argentina’s Personal Data Protection Act, 2000 states that only if prior consent is taken from the subject, personal data can be handled or processed. Individuals also have the right to access, modify or delete the data as per their convenience.
2	Brazil (https://content.next.westlaw.com)	Brazilian Internet Act, 2014 states that privacy policy must be easily understandable and accurate to the users. The policy should include terms and conditions for data collection.
3	Hong Kong (https://www.pcpd.org.hk)	Hong Kong’s Personal Data Ordinance states that any violation of privacy leads to a fine of HK\$50,000 and imprisonment of 2 years.
4	India (www.dot.gov.in)	The Information Technology Act states that every organization has to publish its privacy policy on its website. It is also stated that they will never take passwords or financial information at any point of time.
5	Japan (http://www.cas.go.jp)	The Personal Information Protection Act protects the personal data under the right of individuals. The act states that personal data collection purpose should be well defined and should not be shared without prior consent.
6	Mexico (http://media.mof.go.com)	The Federal Law for the Protection of Personal Data Processed by Private Persons deals with privacy of individuals data. Data can only be collected

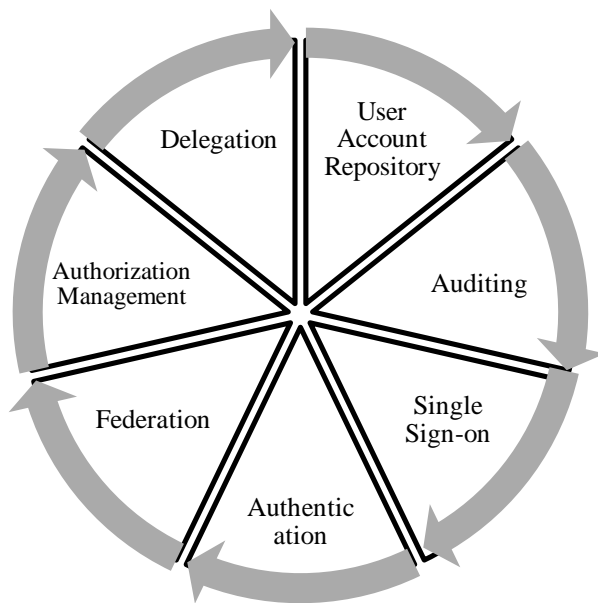


Figure 1: Process and Components of Identity Management

Privacy is defined as the wish of a person to control the personal information from revelation [4]. All the countries in the world are having their own regulations and laws to protect privacy of their citizens. Organizations like facebook, google, yahoo, twitter etc have to obey these legal conventions to ensure customers privacy protection. Privacy is defined in five major dimensions as query, identity, location, owner and footprint [5]. There are privacy protection tools available for customers like Extended Privacy Definition Tool (ExPDT). There are beneficial to organizations also as they act in accordance with with latest regulations and rules [6].

		for the reasons mentioned in privacy policy. Also, organization has an obligation to inform users.
7	New Zealand (http://www.legislation.govt.nz)	New Zealand's Privacy Act of 1993 states that data may be collected by law or any personal reasons. But individuals must know the name, address and purpose of data collection agencies.
8	Singapore (https://www.pdp.c.gov.sg)	The Personal Data Protection Act of Singapore states that personal data should be collected only with prior consent and purpose defined to individuals.
9	South Africa (http://www.inter.net.org.za)	Electronics Communication and Transactions Act states nine principles that an individual should agree then only the personal data can be collected.
10	United States (https://www.hhs.gov , http://www.coppa.org/ , http://consumercal.org)	US has three main privacy protection acts i.e. Health Insurance Portability and Accountability Act of 1996 (HIPAA) which applies to health related information, Children's Online Privacy Protection Rule (COPPA) which deals with collection of data from children under the age of 13. California Online Privacy Protection Act (CalOPPA) includes information on the type of personal data collected, privacy policy implementation effective date.
11	United Kingdom (https://ico.org.uk)	The Data Protection Act states that every organization must upload information related to rights of individuals in public interest.

Also the amount of digital identities per person has increased in last few years. Kumar & Pradhan [7] have evaluated the benefits of social media marketing in different fields.

The main benefits of social media marketing to organizations have increased exposure of products to customers is 90 percent

and increased traffic is 77 percent. However, with the growth of social media, the competition has also increased worldwide. This has introduced a huge challenge of customer retention and customer satisfaction. Trust management is studied from different existing models which will facilitate organizations to develop user trust and increase businesses using social media. Social media here is a system, which allows market forces to engage, collaborate, interact and use intelligent sources for marketing purposes. Kumar & Pradhan [8] have discussed the composition and requirements of the Service Level Agreements for SaaS environments. The most focused SLA is found by analyzing different services [9]. This includes social media services, e-mail services and commercial services. With the increasing number of online identities, the SLAs are becoming more and more complex with increased challenges. This has also introduced the requirement of new challenges to the SLAs for next generation services. The importance of SLAs can be understood from different perspectives such as cost parameters, quality of service, list of services, direct interaction, availability, reliability, performance and security. It has been found cloud based ERP solutions as best in present market scenario of ubiquitous portable devices such as laptops, tablets and smart phones. They have also studied the performance of frequently available clouds in three different locations of the world. This has determined their performance region wise so that their selection can be done based on performance in that region. The comparative study of cloud ERP is done for Avanade Cloud ERP, Acumatica, NetSuite ERP, Microsoft Dynamics, Intact and myERP. In 2016 presidential candidate Donald Trump was hit by many fake accounts.

III. CHALLENGES FOR USERS AND BUSINESSES

Users can have access to applications via a WiFi network, Internet TV, mobile with iOS or Android at home or at office [10-13]. They want data at a faster speed and without any overheads.

Increasing cost: Increase in help desk calls of customers for support or feedback. More work for security administrators is one the main user challenge when concerning identity management. Increasing cost is one of the bottlenecks in most of technology advancements.

User security: Users with many security entitlements and unreliable access restriction forms a major challenge to identity management. There are many security threats associated with security like spoofing, tampering, repudiation, information disclosure, denial of service and elevation of privilege.

Services to user: Users have to wait for passwords and access rights in getting services of identity management which forms a bottle neck. The users may lose temperament for identity

management and thus should be resolved earlier. Availability of services every time, everywhere and through web is major challenge.

Business users:

Users are always having an increasing demand for accessibility and priority of spending less money on applications. Portability is one issue which shifts customers to other organizations with more features.

IT Support: Businesses has to provide Information Technology support for user access to systems. This is done while maintaining security, enhanced features and responsive user services. Most of the applications are running on web or mobile based operating which makes IT support most important.

Audit: Audit is done to verify that user has not done any unauthorized activity. Moreover, it can also be carried out for forensic analysis, if required in any offence. Organizations are also being checked for any misuse of information related user attributes like passwords, age etc. Privacy of users can be maintained through audit.

Business units: They want maximum users to access their applications for which agility, advertisements etc, are formed. Earning profits for their share holders is the main parameter of importance. Identity management provides features like authentication, authorization, provisioning and scalability to attain the same.

IV CONCLUSIONS


The paper concludes the user and business challenges for successfully deploying identity management systems. This will help in gaining maximum benefits and reducing the overall costs. The challenges which can be tackled includes increasing costs, user security, services to user, business user requirements, IT support, audit and different units for authentication, authorization, provisioning and scalability.

REFERENCES

- [1] Horn, G., Moeller, W. D., & Rajasekaran, H. (2017). *U.S. Patent No. 9,749,309*. Washington, DC: U.S. Patent and Trademark Office.
- [2] Jones, M. R., & Karsten, H. (2008). Giddens's structuration theory and information systems research. *MIS quarterly*, 32(1), 127-157.
- [3] Pato, J., & Center, O. C. (2003). Identity management: Setting context. *Hewlett-Packard, Cambridge, MA*.

- [4] Martínez-Ballesté, A., Pérez-Martínez, P. A., & Solanas, A. (2013). The pursuit of citizens' privacy: a privacy-aware smart city is possible. *IEEE Communications Magazine*, 51(6), 136-141.
- [5] Kähler, M., & Gilliot, M. (2009). Extended Privacy Definition Tool. In *PRIMIUM* (pp. 43-59).
- [6] Kumar, V., & Pradhan, P. (2015). Trust Management Issues in Social-Media Marketing. *International Journal of Online Marketing (IJOM)*, 5(3), 47-64.
- [7] Kumar, V., & Pradhan, P. (2016). Reputation Management Through Online Feedbacks in e-Business Environment. *International Journal of Enterprise Information Systems (IJEIS)*, 12(1), 21-37.
- [8] Greschbach, B., Kreitz, G., & Buchegger, S. (2012, March). The devil is in the metadata—New privacy challenges in Decentralised Online Social Networks. In *Pervasive Computing and Communications Workshops (PERCOM Workshops), 2012 IEEE International Conference on* (pp. 333-339). IEEE.
- [9] Takabi, H., Joshi, J. B., & Ahn, G. J. (2010). Security and privacy challenges in cloud computing environments. *IEEE Security & Privacy*, (6), 24-31.
- [10] Vidyalakshmi R. and Kumar V. (2016). Challenges in Implementation of Cloud Analytics. *IPASJ International Journal of Information Technology (IIIT)*, 4(6), 7-13 (ISSN 2321-5976).
- [11] Weber, R. H. (2010). Internet of Things—New security and privacy challenges. *Computer law & security review*, 26(1), 23-30.
- [12] Yang, K., Zhang, K., Ren, J., & Shen, X. (2015). Security and privacy in mobile crowdsourcing networks: challenges and opportunities. *IEEE communications magazine*, 53(8), 75-81.
- [13] Zissis, D., & Lekkas, D. (2012). Addressing cloud computing security issues. *Future Generation computer systems*, 28(3), 583-592.
- [14] <http://www.cas.go.jp> [01.05.2018]
- [15] <http://www.coppa.org/> [01.05.2018]
- [16] <http://www.internet.org.za> [01.05.2018]
- [17] <http://www.legislation.govt.nz> [01.05.2018]
- [18] <http://consumercal.org> [01.05.2018]

- [19] <http://media.mofo.com> [01.05.2018]
- [20] <http://unpan1.un.org> [01.05.2018]
- [21] <https://content.next.westlaw.com> [01.05.2018]
- [22] <https://ico.org.uk> [01.05.2018]
- [23] <https://www.hhs.gov> [01.05.2018]
- [24] <https://www.pcpd.org.hk> [01.05.2018]
- [25] <https://www.pcpd.org.hk> [01.05.2018]
- [26] <https://www.pdpc.gov.sg> [01.05.2018]
- [27] www.dot.gov.in [01.05.2018]

	<p>Aashish Bhardwaj received his Master of Science in Electronics from Kurukshetra University, Haryana, India and further Masters in Technology in Computer Science and Engineering from the same University. He is a member of Indian National Science Congress Association, Indian Society for Technical Education, Institute of Electronics & Telecommunication Engineers and Computer Society of India and has contributed many research papers to reputed journals and conferences. Presently, he is working for PhD degree in Computer Science & Engineering from Mewar University, Chittorgarh, India.</p>
	<p>Sarvottam Dixit is working as a Professor in Department of Computer Science & Engineering, Faculty of Engineering & Technology, Mewar University, Chittorgarh, Rajasthan, India.</p>